PRIVACY AND THE MANAGEMENT OF (DATA) SECURITY

by Kristo Ivanov

ABSTRACT

This tutorial paper summarizes some current thoughts on data-security and considers the problem of its managerial evaluation in terms of three basic approaches: practical, decision-theoretical, and systems-analytical. The conclusion is that some present practical approaches require a stronger rational basis as an insurance against future failures. There is weak evidence for the claim that present data-security efforts will enhance a vaguely understood privacy. Data security may not be separable from other security and confidence in predictions: it may turn out to be an unfortunate concept which is intractable with scientific method. Scientific and ethical considerations suggest that security itself will become more meaningful if it is framed in terms of the alternative concept of accuracy. Privacy has more to do with freedom of expression and civil rights than with confidentiality, authorization and isolation.

INTRODUCTION

The development of large-scale data-processing applications with multiprogramming and remote time-sharing techniques has been followed by a wide concern for personal privacy, organizational privacy or exposure to economic losses, and related security issues.

The evaluation of attained level of data-security is obviously of fundamental importance in controlling activities where investments totaling an amount of the order of magnitude of hundred million dollars are being made with the purpose of attaining better and more data-security.

What is data-security? There are today many practical approaches to this question, which are partially documented in the literature. [4].

SECURITY AS A PRACTICAL CONCEPT

1. The most common present understanding of data-security is in terms of relationships to other concepts of the broad socio-political debate. For example data-security is seen as the technical means of implementing confidentiality. Confidentiality specifications or clearances are in turn the concretization of privacy requirements in terms of "status or levels of sensitivity" of data items, how and what information will be collected, how and by whom it will be used, how it can be reviewed, modified or corrected. Privacy, confidentiality, and security are said to correspond respectively to the philosophical, legal, and technical aspects of a subject's interaction with a databank system. The subject is a person or organization about whom data are stored in the databank system.

The ability to insure confidentiality is then seen as a prime tool in the protection of privacy. Such ability would be the function of data security, which implements confidentiality by protecting information from the threats of unauthorized intentional or accidental modification, destruction and disclosure.

This may be compared with the stated purposes of the overall security program of an organization: Prevent the loss of assets, limit or constrain the magnitude of the loss, and recover from loss. Other common statement of purpose include the protection against intrusion or intruders.

2. Data-security is also seen as being in some sense composed of confidentiality and quality, which together with legitimacy sum up to privacy. Legitimacy

(or "appropriateness") is a moral, legal, and political question while confidentiality and quality are technical and administrative questions. Society's political and legal tolerance is seen as a function of security and legitimacy in the sense that there is a tendency to declare illegal databanks which operate with low degrees of legitimacy and security.

3. Data-security has alternatively been defined in terms of being a component of the broader computer-security program which in turn is one aspect of the overall security of the organization for protecting people, facilities, and data from natural and man-made hazards, e.g. against fire, water, organized crime, etc.

Data-security is also defined in terms of its own contents e.g. specifying that it includes far more than e.g. access-control mechanisms intended for time-sharing with remote terminals.

A related more detailed approach has also been to define data-security or more appropriately EDP-security in terms of its structure along the 2 dimensions of purpose and part or place the system where the counter-measure is implemented. The purpose of security may then be subdivided in physical (protection of physical assets), functional (equipment reliability), data access-control, and quality-control. The parts of the system can be the environment, hardware, software, and the organization.

An alternative related approach is the listing of 4 gross categories of things required in any system, for a systematic procedure to appropriate security measures: identification, authorization, audit, and system integrity.

4. Data-security is furthermore defined as a function of what does affect security, i.e. as a function of threats and countermeasures. Classes of countermeasures, e.g. legal sanctions, cryptographic transformations, access control, etc. are referred to as belonging alternatively to environment, hardware, software, or to organisation-administration.

5. Data-security is defined in terms of the type and quantity of resources which are required in order to "break the security wall" or, more generally, to inflict a loss. Three types of mentioned resources are knowledge of hardware, software etc., collusion or cooperation among key personnell who control system resources, and necessary time.

6. Data-security is finally also defined by physical analogy to e.g. protection from rain by means of umbrellas, from thieves or fire by means of vaults and safes, and from enemy-attacks by means of a protecting fortress.

The above conceptualizations of data-security are intuitively appealing but they are not "safe" since they are not explicitly related to scientific method. They may convey a confusing feeling of incompatible "ad-hoc" approaches. The reader may check this by attempting to express the proposed definitions in a logical-mathematical notation. They are not yet in an operational form supporting the evaluation of the attained level of security, i.e. the common criterium for usefulness and choice of definitions.

The concepts are very complex indeed: the use of the same word often refers unintentionally to different things. For example one has the privacy of a person (or of an organization). Security of the machine (or of a software technique, or of the "system"). Protection of privacy (or of information, of physical assets, of confidentiality), etc.

The above ambiguities and questions, however, have not prevented the creation of practical-empirical security programs. Such programs or efforts assume that even if security is not yet understood, there are many things which can be done, i.e. many counter-measures which can be designed and implemented.

Let us therefore look next at the status of the design of security.

The design of data-security as opposed to the definitions considered above is claimed to be characterized by additional consideration to costs, negative values, and constraints. The formulation sometimes is that the creation of design criteria is the question of relating countermeasures to some level of system security: how good is the developed countermeasure, how good it should be. Among design criteria are listed effectiveness, economy, simplicity, and reliability.

Among costs for implementing a data-security system are mentioned those for planning and design, investment in hardware and software, recurring operating costs, and decrease in functional capability.

Design is then considered as synonymous to rational approach to implementation as opposed to the "social policy approach" which is equated to protection at any cost.

Present activities going on in industry and administration, however, suggest the further existence of some kind of design of design in the sense of creation of more general countermeasures or methods of protection for threats in different classes of operating environments. The goals of such design emphasize costs and are said to be e.g. the development of countermeasures and the measurement of their costs, to develop methods for estimating the costs of implementing safeguards in various classes of information systems, to investigate the applicability of fitness of protection-methods, or even to contribute to the overall goal of protection against threats. The generality and vagueness of such claims stand in sharp contrast to the requirements of practicality and concreteness which are invoked for justifying the disregard of theoretical and methodological issues.

From the management point of view, however, the measurement of costs is not sufficient for managing the design effort especially when no concrete results are reported in terms of attained levels of security. Effectiveness is generally understood as a relationship between benefits and costs, positive and negative values. Management therefore requires that benefits or positive values also be measured. Furthermore it is not clear what does it mean to include e.g. effectiveness among the goals of the system. It amounts to state that the one of the goals of the system is to attain the goals at minimum cost which, considering that costs represent some of the system constraint-goals, does not throw more light on the nature of the goals, and displays a certain circularity of reasoning.

Management may indeed meet difficulties in evaluating the implementation and the design of security based on the above statement of goals. How good is a developed method compared with another method? Is it possible to reduce the solution of the security problem to the writing down of a list of possible threats and to specify one countermeasure for each threat? How good or effective is the implemented method? Is it meaningful to separate the evaluation of design from the evaluation of implementation? Since data can represent other assets, by manipulating data the other assets might be manipulated maliciously: is it useful to conceptualize objects as distinct from data about objects? Does this affect the separation of data-security from other security? It is not clear which is the relevance of physical analogies to data security, e.g. in terms of safes. How to evaluate the implications of the fact that sometimes the locking of valuable things in a safe may lead to greater total loss caused by a determined intruder who damages both the door and the lock?

It may be impossible to talk about the effectiveness of a countermeasure or method without relating it to security, i.e. without discussing the costs and values of its implementation. This is particularly evidenced when attempting to discuss the effects on security of e.g. geographical centralization-decentralization of EDP-hardware. This means that the evaluation of the security system must include both the design and implementation steps, and it must essentially consist of decisions based on relations between threats and countermeasures.

The practical approaches raise many questions without offering any scientific justification i.e. reason for having confidence in the results. We will therefore attempt to simplify and conceptualize the security problem in terms of decision theory as a means for evaluating some of the implications of the practical approach.

SECURITY AS A DECISION

Instead of starting with intuitive practical definitions of security we state that it represents a problem. To solve a problem is to make the best choice from among the available courses of action. [1, 14]. Any problem situation can be represented by the equation V=f(X, Y) where V is measure of performance, accomplishment, or effectiveness that we seek to maximize, X is the set of variables or aspects of the situation affecting V which the we can control, Y is the set of variables or aspects of the situation affecting V, over which we have no control (i.e. the environment of the problem).

The most simple type of problem involving two possible outcomes, both qualitatively defined, and two available courses of actions or strategies can be represented in matrix below. Let X1 and X2 represent the courses of action or strategies corresponding to set X, Y1 and Y2 represent two possible states of nature or competitor's actions or states of environment corresponding to set Y, O represents the physical description of the outcomes (e.g. in terms of inputs and outputs), P is the probability of O being produced by X under state Y, V represents the relative values of outcomes to the decision maker, i.e. the value of products minus cost of consumed resources.

		States of nature	
		Y1	Y2
Courses of action	X1	(O11, V11, P11)	(O12, V12, P12)
	X2	(O21, V21, P21)	(O22, V22, P22)

It is now obvious that security can be conceptualized as a decision problem: Threats, if anything, may be identified as e.g. states of nature, while countermeasures or protective measures may be identified as courses of action or strategies. It is also apparent that the lack of such a conceptualization up to now has resulted in definitional problems for the security area. For example O is equated with V, V is equated with the cost of X, Y is equated with O. New vague concepts are consequently created such as (value of) attained level of protection, amount of security provided, need of protection, (value or cost of) potential damages, value of countermeasures, cost of implementing security barriers, value of decreased probability of damages, value of damages which could be caused by defective protection of data, probability of damages which may occur at a given level of protection, relative risks or costs for various possible damages, etc. Such concepts introduce in turn the need for models about e.g. the relationship between value of information to the involved parties, the cost of protection, cost of intrusion, and the effectiveness of data security and intrusion techniques.

The representation of the security problem as a decision suggests that it may be considered under conditions of risk (as in the above matrix), or uncertainty whenever the probabilities are unknown or when the states of nature represent competitive strategies of a rational opponent. It is interesting to note that economic models of protector-intruder strategies have not been framed in terms of game theory, and that at the same time the present "military" approach has not emphasized models for evaluation of countermeasures against non-competitive or accidental threats which may be the most common in civil applications.

An additional insight is that decisions under certainty, risk, and uncertainty may be related to the three basic scientific approaches which are consistent and interdependent: deterministic, probabilistic, and teological or purposeful. In the security area the problem has been intuitively or unconsciously rephrased in terms of accidental versus intentional threats which are apparently considered as complementary and independent. The deep methodological problems in the measurement of probabilities present difficulties which may easily be underestimated.

The formulation of security as a decision problems suggests, furthermore, that some of the definitions referred to at the beginning of this paper may have resulted from an unconscious attempt to cast security in decision terms.

The conceptualization of security as a decision or choice about countermeasures has the embarrassing consequence of pointing out the need of estimating both implementation costs and benefits of countermeasures. The question cannot be evaded by equating benefits to the decreased expected losses (or decreased probability of losses) compared to losses which would be incurred with no countermeasures. This is so because the estimation of costs presumes some model or else the decision model should assume that the zero alternative, i.e. no countermeasures is also represented by a row-entry in the above matrix. The costs and benefits of the zero-alternative are also relevant and must be known unless one can prove that benefits are the same for all alternatives. Comparison between the zero alternative and other courses of action must be made on the basis of comparing the net values of their outcomes, or at least by comparing the outcomes themselves (and their costs) in terms of reliable measurements of specific physical variables.

Another attempt to avoid the burden of accounting for benefits is to state that benefits derive only from the implementation of countermeasures while the concerned program aims only at the design of countermeasures and determination of their cost. The approach, however, leads to a regression to another decision problem, i.e. the choice of the best design procedure, where the outcomes with their respective values are the design specifications. Rational design must be a design up to specifications.

Still another attempt to justify some present practical data-security approaches is to see the design problem as design of one countermeasure for each type of threat. This is sometimes done by identifying discrete "objects" which are then called resources or assets, assigning to them a value which is equated to the cost of exposure (e.g. equated to its worth to an intruder or cost of replacement) and estimating the probability of such an exposure. The design of countermeasures will then give higher priority to those threats with high expected value (cost).

possible acquisition of this information by the intruders. Nevertheless the problem of accidental disclosure to potential intruders will require some integration of the different decision models. Other conceptual difficulties are uncovered by the use of the concept "resources". Resources are used to protect recources. This calls our attention on the need to define the concept of resource and on fact that we are indeed confronted with a systems-problem which could be attacked through modern systems analysis techniques, i.e. generalized decision models.

With this purpose in mind we start observing that the present approach to data-security presumes indeed the following idealized decision situation, with weak interaction between different threats and with highly selective effect of countermeasures.

		Threats			
		Y1	Y2	Y3	Y4
Counter-measures	X1	V1	-	-	-
	X2	-	V2	-	-
	X3	-	-	V3	-
	X4	-	-	-	V4

The total expected value of the data-security program is then roughly $E(V)=E(V1) + E(V2) + E(V3) + E(V4)$. If some interactions are stronger than other, sets of countermeasures can be grouped under unique functional responsibility, e.g. security-department D12 of the firm performing actions X1 and X2 aimed at environments Y1 och Y2, and security-department D34 aimed at Y3 and Y4, with V12 och V34 being the measures of performance aimed at the desired levels, or goals.

The striking implication of this approach is that we are formulating a decision based on only one alternative (besides the zero-alternative), or equivalently we formulate a solved system as composed of subsystems. The given threats have the same conceptual status as other given environments of the organization Y5, Y6 etc. What does distinguish (data-)security from other organizational goals such as sales and production and why no attempts are made to integrate security with the systematic approach to other economic and organizational problems? On what basis to decide between the proportion of resources to be allocated to physical protection of a terminal, to software protection of a data item or an account receivable file, and to research and development aimed at increasing the receivable assets and hence increasing the value of the accounts receivable file to be protected in the future?

The need of integration of security with other organizational problems is also evidenced by the possibility of regarding V1, V2, V3 and V4 in the previous figure as different objectives of the firm. V1 could be sales, V2 goodwill, V3 security, and V4 production, as an example. V3 stands just for some specific kinds of values which must be balanced against other values, where values may relate to different people in the organization or in society. What is security, after all, and <u>why</u> is it so defined?

The system-organizational character of the problem is also uncovered in some present economic models of protector-intruder strategies. It is stated e.g. that the expenditure of resources or investment for data-security measures should reflect the value of the protected information to the subjects about whom the data is stored, value to the protector himself, and value to potential intruders.

The cost of threat to the intruder should then be higher than the value of information to him, and also higher than his opportunity cost for obtaining the information from other sources. In an analog way the cost of protection to the protector or custodian, and to the subject should be lower than the (negative) value or cost of the potential damage to him.

The advantage of the earlier proposed conceptual-ization in terms of a decision problem is that it shows that the presently proposed alternative is limited to the game-theoretical context of strategies against a rational opponent.

		Intruder	
		Y1	Y2
Protector	X1	V(X)11, V(Y)11	V(X)12, V(Y)12
	X2	V(X)21, V(Y)21	V(X)22, V(Y)22

Y is the set of threats-actions and X is the set of protection countermeasure-actions. V(X)11 is the value to the protector, of the outcome of his choice of countermeasure X1 and the intruder's choice of threat Y1. Such value should represent the benefit minus the cost of X1. Sometimes it is claimed that the value to the protector is equivalent to the cost to the intruder. This would imply a zero-such game. However, <u>more generally</u>:

$$V(X)11 = B_X(X1, Y1) - C(X1)$$

and similarly $$V(Y)11 = B_Y^X(X1, Y1) - C(Y1)$$

where V(Y)11 is the value to the second decision maker of the outcome resulting from X1 and Y1.

The solution of such problem in its general form is the task of modern economics and systems analysis. It is not clear whether the simple decision approach to data-security is fruitful besides of ordering the used concepts and suggesting its own limitations. At any rate it is obvious that the game-theoretical variant suggested above is not neither intended for economic analysis of so-called accidental threats, nor for management evaluation of the (data-) security program.

Most of the unsolved problems appear to be centered on the identification of relevant human actors, definition of variables and measurement of values.

SECURITY AS A SYSTEM

The systems approach can be regarded as a generalization of the decision-theoretical framework for decisions under certainty risk and uncertainty, both against "nature" and rational opponents. If furthermore may allow an integration with economic theory and modern organization theory. [5, 6] .

We start from the basic formulation of the problem situation V=f (X, Y). This corresponds to a decision function for which we have defined the (security) measure of performance V, as a function of the resources or controlled variables X1 and of the given environment or parameters Y1. The extension of the earlier stated "physical" decision problem to an economic and organizational system emphasizing the involved humans requires the qualification of who is "we", i.e. the additional definition of a decision maker, manager, controller or influential subject who represents identified clients of the system in terms of the measure (value) of performance. It also requires the definition of the system components or subsystems represented by decision makers who use up the system resources assigned to them by the management in order to perform the activities of the system.

Resources are defined as what is under the control of the decision maker in the sense that he can allocate them for consumption by the subsystems in the pursuit of the subgoals which must be consistent with the system's goals. Environment is the correlate of the resources and together with them it implies a definition of the limits to "givens" of the system. Environment is everything which can affect the system's performance as seen by the legitimate clients of the system, but is not under the control of the decision-maker.

The earlier protector-intruder model turns out to be a simplified conflict-game version of a system with 2 components, where the total system measure of performance is practically identical to the protector component and system activities are reduced to threats and countermeasures. The present social system formulation, however, seems to be necessary whenever the resources invested in security are so large that they become of social concern, outside the strict limits of technically oriented small "unique-component" private business. Then it really matters what is meant by "security", and "whose" security!

Two possible visual representations of the security problems are presented below. The first is the most common and prevalent today. It is a "databank system" cast on terms privacy around the subject; confidentiality around the collector, custodian, and databank; data security between the databank and the intruder. The databank system has been considered as composed of subject, controller, collector, custodian, databank, user, intruder, and society. [8].

The second figure is an alternative tentative partial visualization of the same "system" in terms of the social system approach proposed above.

In the second social-approach figure, society is composed of users-decision-makers A, B, C, etc. e.g. respectively protector, intruder, and controller. PL(A) stand for the product line of the protector who produces information outputs such as descriptions of manufactured products or of software countermeasures P(A). Such production according to technology PL(A) requires the use of resources R(A) (which imply costs C(A)), within the constraints of the environment E(A) e.g. location and nature of physical facilities, processing environment e.g. batch, interactive, remote job entry, etc. The resources of A are defined as what he can control, while the environment is what he cannot control but still affects the value V(A) of the product P(A). In particular the resources of B, especially if B is a conflicting intruder, may be a part of E(A).

The use of P(A) leads to benefits which together with the cost C(A) lead to the final value V(A) according to some cost-benefit computation V=f (X, Y), in particular V(A)=f (R(A), E(A)).

V(A), and the analog V(B), V(C) etc. sum up to the "larger system's" or to society's (security) value V(S) which is legally defined by the controller C. The figure indicates that the controller has the very delicate specific function of defining the function "f" on behalf on other society's members such as users A and B. A meaningful measure of privacy and security may then be represented by the accuracy in the determination of the V's and other variables of the social model. A subject's privacy-interactions with society obviously require a much more complex model. [2]. The concept of privacy has indeed little in common with simple mechanical and military analogies, intrusion, isolation, confidentiality, authorization, etc. It appears rather associated to subjectivity and synthesis in science as related to the concepts of objectivity and analysis. In the legal context, privacy has been sometimes translated to other languages as integrity.

In the context of the alternative model proposed above, the evaluation of some approaches to protector-intruder economics seems to be a trivial thing. One approach mentioned earlier requires that e.g. V(A) and V(B) be positive, and that C(A) and C(B) be smaller than the opportunity of R(A) and R(B) (i.e. values for other users of the system - subjects who have a legitimate expectation of deriving benefits from the system). But this formulation is just a variant of suboptimization together with a reformulation of the basic system problem of "opportunity costs".

The attempt to evaluate security indicates once more that it stands for somebody's specific values among many others in the system. Or then all values are security in the sense that the system aims at securing the attainement of the multiple goals. Security variables can only be evaluated through the use of some model. The only security in passing a bridge is the security of the computation of the critical variables in the model of its structure, based on the security of the estimation of environmental parameters. It may not be meaningful to distinguish objects from data about objects, security of bridge from security of computations about the bridge, security of the activities affected by the computer (e.g. privacy) from security of data about the activities or from security of the computer[1].

It is just the case that data about physical concepts are often called objects while no special "nickname" is used for data about other than physical aspects of reality, e.g. economic, psychological and social concepts. Physical concepts are not more "real" than other concepts. Objects are themselves concepts, i.e. data.

All this is perhaps a new aspect of the old methodological truth stating that data cannot be separated from their use. The matter has certain obvious implications for the security of databanks not developed within a systems approach, as well as for the uses to which security will be put e.g. protection of privacy. These insights should definitely relieve the privilege that security has of being treated in terms of threats and countermeasures. It may turn out to be a semantic escape to the issue of value measurement and rational estimation of benefits. Whose threats, and what threats to whom may become a issue of great concern which may be equivalent to the issue of costs and values. And the problem of who, whose, and whom are clearly related to privacy. This implies that present investments in data-security rather than in data-accuracy and in a methodology for social systems analysis, may be implicitly biased towards certain values: recent sociological analyses also suggest that data security may not exist as a neutral tool at the service of privacy. [9].

CONCLUSION: SECURITY AS A MYTH

The foregoing suggests that the present emphasis on security may constitute a modern expression, the latest expression of the myths which deal with human fear and anxiety. Mythology is becoming a rich source of knowledge on the problems of systems analysis.[6, 11, 15, 16] Myth is not a lie. Webster's Third New International.

Dictionary offers, among others, the following definition of myth: "a belief given uncritical acceptance by the members of a group esp. in support of existing or traditional practices and institutions". Security may inadvertedly be substituing man's search for God, Truth, and Efficiency, in that order.

It is possible that security, particularly in its relationship to citizen privacy and integrity, should be reduced to the traditional scientific concept of accuracy which, however, must be redefined for the social context. [13]. Scientific method was indeed created by man as one way, the "rational" way, for dealing with anxiety and fear by means of (accurate) predictions of the future.

Perhaps the only meaningful security in this world is then the security of the answer to certain questions, e.g. "how secure or valuable is this system?" and this is equivalent to the accuracy of the answer within the frame of certain models. Such formulation substitues security as function of confidentiality and authorization, with accuracy as a function of openness and negotiation where civil liberties are a fundamental requirement. There are some signs that suggest such shift of emphasis. [7, 8, 9, 10, 19]. The relationship between force and understanding or the role of military and police (and security officers) is central to social systems analysis. [3].

A curious most important implication is the recognition that security is in some sense opposed to accuracy. If the information is kept more confidential, it also gets less challenged, more doubtful information will be likely to be recorded and used, and this corresponds to a loss of control on it, i.e. decreased accuracy. Better accuracy and "truth" may imply decreased probability of, and losses from intrusion. [10]. This interpretation is obviously related to the freedom of the press and civil liberties as well as to parallel thoughts in the field of national security, law and public administration. [7, 8, 10]. This may be the solution of the apparent conceptual conflict between privacy and democracy: data banks, if created at all, must be designed to handle conflicting estimates and disagreements. [9, 13].

The specific formulation is mainly of "academic" interest so long as people do not care. This may come soon to an end to the extent that increasingly significant societal resources are allocated to data-security, and to the extent that public debate returns to emphasizing privacy and social values instead of security.

From the managerial point of view taken in this paper it is difficult to be more concrete at this point in time since we do not know of any concrete security results reported by the technological community. By concrete result here we mean a substantiated statement at least in the form e.g. "This system has a security level as defined by the following set of variables which are guaranteed to stay within the following tolerance limits..." Some recent attempts to develop practical computer-secure models are indeed very "theoretical" and may be interpreted as a modern variant of sterile logical reconstructionism as the term has been used in the literature on scientific method.

This uncovers important practical problems which also appear in connection with present increasing use of such concepts as identification, authorization, authentication or authorization of the identification, identification of processes, identification by people versus identification by computers, etc. Other problems are also evidenced by the difficulties of present privacy-security approaches in dealing with certain specific issues. E.g. the determination of "sensitivity-level" of data depends upon how it is used by whom; data may be not sensitive but aggregations may turn out to sensitive and dangerous; privacy may be hurt by non-personal information; etc. Why should we believe that privacy will be protected by means of confidentiality and anonymity? Furthermore, earlier in this paper we mentioned the difficulty to evaluate the dependence of security on centralization-decentralization policies.

The issue no doubt implies a future challenge to sociologists, political scientists, managers, and civic leaders outside the restricted community of lawyers, mathematicians, statisticians, and computer professionals who have dealt with the privacy problem up to date. The challenge is not hopeless to the extent that we dispose of a platform for the development of a socially oriented methodology of systems analysis [2, 5, 6]. Certain extensions of game theory and its linkage to economic theory may also be useful for helping to realize the limitations of simple decision models. [17].

The path to be followed is probably to abdicate from the myth of security and return to the old quest for accuracy, scientific method, and purposeful inquiry. The path will be painful because it implies abdication to a sense of (false) security. Scientific security or truth was never based on confidentiality and authorization.

The manager's integrity will have to be very high indeed if he is going to refuse allocating resources to try to prevent something which may indeed happen as result of his prior investment decisions, and endanger his political position in the organization, just in order to allocate them to something more valuable.

REFERENCES

1. ACKOFF, R.L., Scientific Method: Optimizing Applied Research Decisions, John Wiley, 1962

2. ACKOFF, R.L. AND EMERY, F.E., On Purposeful Systems, Aldine - Atherton, 1972

3. BOGUSLAW, R., "Systems Concepts in Social Systems" in R. Miles (ed.) Systems Concepts, Wiley, 1973

4. CANNING, R.G., "Protecting valuable data", EDP Analyzer, 11,12 and 12,1 (December 1973, January (1974)

5. CHURCHMAN, C.W., The Systems Approach, Dell Publishing Co., 1968

6. CHURCHMAN, C.W., The Design of Inquiring Systems: Basic Concepts of Systems and Organization, Basic Books, 1971

7. CLEVELAND, H., The Future Executive, Harper & Row, 1972

8. CLEVELAND, H., "Systems, Purposes, and the Watergate", Operations Research, September-October 1973

9. EHN, P., Contributions to a Critical Social Perspective on the Development of Computer-Based Information Systems, (in Swedish), Dept. of Administrative Information Processing and Computer Science, University of Stockholm, 1974

10. GRIP, A. AND IVANOV, K., The Influence of Governmental EDP-Systems on Public Administration and on Society, (in Swedish), Report to the Committee on the Coordination and Control of Databanks (DASK), Ministry of Finance, Stockholm, 1974

11. HOOS, I., Systems Analysis in Public Policy - A Critique, Univ. of California Press, 1972

12. IBM Corp., Data Security, Form No. G320-1248-0

13. IVANOV, K., Quality - Control of Information, Ph.D. dissertation at KTH, Stockholm, 1972 (NTIS, U.S. Dept. of Commerce, PB-219297)

14. MILLER, D.W. AND STARR, M.K., The Structure of Human Decisions, Prentice - Hall, 1967

15. MITROFF, I., "The Mythology of Methodology", Theory and Decision 2, (1972) p. 274

16. MITROFF, I., NELSON, J., AND MASON, R.O., "Management Myth-Information Systems", Management Science, in press

17. MORGENSTERN, O., "Game Theory", in P.P. Wiener (ed.) Dictionary of the History of Ideas, vol. II, Scribner, 1973

18. TURN, R. AND SHAPIRO, N.Z., "Privacy and security in databank systems - Measures of effectiveness, costs, and protector - intruder interactions", Fall Joint Computer Conference, 1972, p. 435

19. U.S. DEPT. OF HEALTH, EDUCATION AND WELFARE, Records, Computers, and the Rights of Citizens, U.S. Government Printing Office, No. 1700-00116, 1973

Note 1

The story of science contains several examples of unfortunate concepts which are not tractable with scientific method. Webster's writes about e.g. phlogiston: "the hypothetical principle of fire or inflammability regarded by the early chemists as a material substance", and about ether: "the element formerly held to form the material of the heavenly spheres and bodies from the moon to the fixed stars" or "the upper regions of space or the rarefied element formerly held to fill these regions". The question is whether data security is a kind of phlogiston or ether of the computer age. Does the concept of data security exist? "Is the emperor naked?".